ABSTRACT OF THE DISCLOSURE

Disclosed is a security deciphering apparatus including a hidden secret key storing unit for storing a hidden secret key (Kh) corresponding to intrinsic identification information, a first decoding unit for receiving a personal secret key ({Ks}Kh), generated by enciphering a cipher key (Ks) by using the hidden secret key (Kh), via a public network, and decoding the personal secret key ({Ks}Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks), and a second decoding unit for receiving enciphered data ({M}Ks), generated by enciphering data (M) by using the cipher key (Ks), via the public network, and decoding the enciphered data ({M}Ks) by using the cipher key (Ks), thereby obtaining the data (M). In accordance with the security deciphering apparatus, it is possible to receive data while maintaining a desired security of the data.